Cisco AMP for Endpoints Release Notes

Version 5.4

8 February 2018

AMP for Endpoints Windows Connector 6.0.7

New

- Added /kb4072699 installer switch to automatically set the registry key necessary to receive the Windows Security Update for KB 4072699.

> **IMPORTANT!** Test and ensure compatibility of all AV products installed before using this installer switch. See Cisco AMP for Endpoints Compatibility with Windows Security Update KB4056892 for important details in the Caveats and Considerations section that apply to use of the installer switch for setting the registry key.

Bugfixes/Enhancements

- Improved TETRA file detection parsing. (CSCvh54783, CSCvh77705)
- Addressed an issue where the Connector could cause a blue screen under rare conditions. (CSCvh56811)

16 January 2018

AMP for Endpoints Mac Connector 1.6.0

New

- Added automatic crash reporting.

IMPORTANT! The AMP for Endpoints Mac Connector no longer supports OS X 10.10 and earlier as of version 1.6.0.

Bugfixes/Enhancements

- Fixed a bug that caused retrospective quarantine failure events to be displayed even though it succeeded.
- Improved compatibility with macOS 10.13.
- Updated third-party libraries.
- Reclassified some error messages that were being logged frequently under normal circumstances so they are only seen when running the Connector with Debug Logging enabled in policy.
- Increased the size of the retrospective database from 50MB to 500MB with better pruning efficiency to decrease disk reads and writes.

AMP for Endpoints Linux Connector 1.6.0

Bugfixes/Enhancements

- Improved upgrade process to protect against failures.
- Fixed a bug that caused retrospective quarantine failure events to be displayed even though it succeeded.
- Updated third-party libraries.
- Reclassified some error messages that were being logged frequently under normal circumstances so they are only seen when running the Connector with Debug Logging enabled in policy.
- Increased the size of the retrospective database from 50MB to 500MB with better pruning efficiency to decrease disk reads and writes.

30 January 2018

AMP for Endpoints Console 5.4.20180130

New

- Emails now come from no-reply@amp.cisco.com.
- Redesigned weekly reports with new data summaries.
- AMP Update Server released so you can host TETRA definitions locally and reduce reduce internet-bound bandwidth usage from Connectors. Follow the AMP Update Server Configuration link in Advanced Settings > TETRA in your Windows policies.

5 December 2017

AMP for Endpoints Windows Connector 6.0.5

New

- Exploit Prevention detection engine to block exploits and memory attacks that target certain processes.
- System Process Protection adds protection for memory attacks against certain Windows system processes.
- This version of the Connector runs on Windows 7, Windows 8 and 8.1, Windows 10, Windows Server 2008 R2, and Windows Server 2012. Older versions of Windows are no longer supported.

IMPORTANT! On Windows 7 and Windows Server 2008 R2 you must apply the patch for Microsoft Security Advisory 3033929 before installing the Connector.

Bugfixes Since the Exploit Prevention Beta Connector Release:

- Connector service now functions properly when installed on Windows 10 Fall Creators Update.
- The Connector no longer causes a warning to appear when opening the Computer Management window.

Bugfixes/Enhancements:

- Fixes for multiple ClamAV vulnerabilities.
- Improved security of the Connector Protection password.
- Improved Windows proxy discovery.

- Improvements to make Connector upgrades more robust going forward.
- Addressed an issue where the Connector would leave many temporary files behind, filling up the disk.
- The History page on the Connector user interface now shows the proper detection name for quarantined files that were already in the local cache.
- Improved reliability when an Endpoint IOC scan is launched.
- Updated SQLite version to prevent high CPU usage.
- Improved Connector user interface responsiveness.

IMPORTANT! All upgrades from previous AMP for Endpoints Windows Connector versions to 6.x.x will require a reboot of the endpoint.

AMP for Endpoints Console 5.4.20171205

New

- Added Process Exclusion type to support System Process Protection in AMP for Endpoints Windows Connector version 6.0.5 and later.
- Added Policy settings to enable Exploit Prevention and System Process Protection in AMP for Endpoints Windows Connector version 6.0.5 and later.

IMPORTANT! All policies must be on the new AMP Cloud infrastructure by running the Cloud Migration tool before you can deploy AMP for Endpoints Windows Connector version 6.0.5 and later. All new policies created since February 2016 use the new AMP Cloud infrastructure by default.

Bugfixes/Enhancements

- Added Connector version numbers to the Download Connector page. After you select a Group the Connector version to be downloaded will be displayed for each Connector type.

30 November 2017

AMP for Endpoints Mac Connector 1.5.1

Bugfixes/Enhancements

- Fixes for multiple ClamAV vulnerabilities.
- Addressed memory leak when scanning plist files.
- Fixed potential crash during a failed retrospective quarantine.

AMP for Endpoints Linux Connector 1.5.1

New

- Official support for RHEL/CentOS 7.4.
- Official support for RHEL/CentOS 6.9.

Bugfixes/Enhancements

- Fixes for multiple ClamAV vulnerabilities.
- Fixed HTTP parsing for certain processes.

28 November 2017

AMP for Endpoints Console 5.4.20171128

New

- You can send users a notification to set up Two-Step Verification.
- New filters added to Users page: Last Login, Two-Step Verification, Remote File Fetch, and Command Line.
- A CAPTCHA is displayed when a user has many failed login attempts.
- New UI for improved Policy configuration.
- Command line data is now available on the API.
- Businesses in the EU can now switch their AMP for Endpoints accounts to use the new EU Threat Grid Cloud.
- Individual users can now be configured with permission to view command line data.
- New popover on clicking IP addresses, URLs, and SHA-256s.
- Enable scanning of Word, PowerPoint, and Excel file types in AMP for Endpoints Mac and AMP for Endpoints Linux Connector policies.

31 October 2017

AMP for Endpoints Console 5.4.20171031

New

- Updated menu colors to be more consistent with other Advanced Threat products.
- Users can now specify Windows 10 as the OS to run analysis on when sending files to the Threat Grid.

- Users can now chose to preview the new Policy UI. The existing policy UI will be deprecated soon.
- Password requirements are now more stringent.
- New Splunk app is now in the Splunk app store.
  https://splunkbase.splunk.com/app/3670/#/details
  https://splunkbase.splunk.com/app/3686/#/details

18 October 2017

AMP for Endpoints Linux Connector 1.5.0.518

New

- Update Linux signed file quarantine guardrail.
- Resume filesystem scans if the daemon restarts.
- Hide exclusion list in UI based on policy configuration.
- Remove old quarantined files automatically.

Bugfixes/Enhancements

- Update 3rd party libraries.
- Bypass proxy when unable to connect to AMP registration server.
- Fix execute not being excluded from scan when it should be.
- Fix custom scan misbehavior.
- Disable unintended auto-start of ampmon after reboot in CentOS 6.
- Scan full contents of archives that contain malware.
- Do not treat directed or scheduled scans which processed zero files as failed.
- Fix restore from quarantine failure.
- Fix CLI crash when displaying very long exclusion lists.
- Fix intermittent failure where CLI is stuck in initializing phase.

17 October 2017

AMP for Endpoints Mac Connector 1.5.0.548

New

- Support macOS High Sierra (10.13).
- Resume filesystem scans after AMP service daemon restarts.
- Hide exclusion list in UI based on policy configuration.

Bugfixes/Enhancements

- Update Third Party libraries.
- Fix memory leak.
- Optimize how exclusions are applied.
- Improve Cloud Recall Restore error handling.
- Scan full contents of archives that contain malware.
- Remove old quarantined files automatically.
- Restrict access permission of some internal files.

5 October 2017

AMP for Endpoints Windows Connector 5.1.13

IMPORTANT! Starting from Windows Connector 6.0.1, we will no longer be supporting the addition of new features for Windows XP, Windows Vista, Windows Server 2003 and Windows Server 2008 (non-R2) operating systems. Critical bug fixes and security patches will still be made to the 5.x.x branch of the Connector for a limited time. For more information, please refer to the End of Support Announcement.

Bugfixes/Enhancements

- Patched a DLL hijacking vulnerability in the Connector installer (CVE-2017-12312).
- Extremely long process command line arguments are now properly captured.
- The Connector UI accurately displays Cloud connectivity status.
- Improved ability of the Connector to detect and repair configuration issues during regular usage and on Connector upgrade.
- Improved performance of Process Exclusions for operating systems prior to Windows Vista.
- Addressed an issue where the Connector is unable to upgrade directly from version 5.0.9 or older to 5.1.11 when Connector Protection is enabled.
- Reliability of Support Package generation has been improved.
- Connector will not generate new identity on machines where the BIOS serial number contains whitespaces.
- Addressed issue where the Connector service does not automatically start after multiple upgrades without a reboot.
- Improved reliability of system reboot after upgrades in Windows Server 2003.

28 September 2017

AMP for Endpoints Console 5.4.20170928

New

- Reorganized top bar navigation:
  - Support link is now in the Help menu.
  - My Account and Log Out links are now located in the new User menu.
- Auto-Refresh on Dashboard - To better help customers viewing the Dashboard on large screens (for example in a Network Operations Centre), the Dashboard page can now be set to auto-refresh.

24 August 2017

AMP for Endpoints Mac Connector 1.4.5

New

- Digitally signed malware will now be quarantined by the Mac Connector.

Bugfixes/Enhancements

- Improved DMG container handling.
- Addressed race condition that would result in failed quarantine restores.
- Custom or scheduled scans that result in 0 files being scanned no longer report as a failed scan.
- Installs of the Connector on a system with multiple users will no longer be incorrectly reported as failed.

9 August 2017

AMP for Endpoints Console 5.4.2017080915

New

- User Name Search feature.
- Allow user to select the AMP Threat Grid VM to use when sending a file for analysis.

Bugfixes/Enhancements

- Fixed a bug in the Product Updates section on the Edit/Create Policy page where Connector version numbers were not sorted correctly.
- Fixed a bug where search results that were shas displayed the incorrect context menu.
- Addressed an issue where inbox events were not grouped correctly.

3 August 2017

AMP for Endpoints Mac Connector 1.4.3

Bugfixes/Enhancements

- Addressed issue where a different folder may be inadvertently deleted during the uninstall process when a subdirectory in the "/Users" directory contains a subdirectory with a space character.

  Note that most systems are not affected as macOS System Preferences prevents creating a user with a space character in the account name.

  To trigger this issue, two similarly-named user directories must exist (e.g. "`/Users/JohnDoe`" and "`/Users/JohnDoe Copy`"). If "`/Users/JohnDoe Copy`" contains the path to AMP Connector log files (e.g. "`/Users/JohnDoe Copy/Library/Logs/Sourcefire/`"), uninstalling or upgrading will result in the user directory "`/Users/JohnDoe`" being deleted.

IMPORTANT! Mac Connector 1.4.2 will no longer be made available in the portal.

If you installed 1.4.2, you must upgrade to 1.4.3 directly without uninstalling 1.4.2.

If you downloaded the 1.4.2 installer, it is recommended that you replace it with a 1.4.3 installer immediately.

AMP for Endpoints Windows Connector 5.1.11

IMPORTANT! Starting from Windows Connector 6.0.1, we will no longer be supporting the addition of new features for Windows XP, Windows Vista, Windows Server 2003 and Windows Server 2008 (non-R2) operating systems. Critical bug fixes and security patches will still be made to the 5.x.x branch of the Connector for a limited time. For more information, please refer to the End of Support Announcement.

Bugfixes/Enhancements

- Updated TETRA license key.

IMPORTANT! The TETRA license for all Windows connector versions prior to 5.1.11 will expire on November 1, 2017. If you wish to continue using the TETRA engine to supplement the cloud-based protection of the Windows Connector, you must upgrade before this date.

- The DFC driver now initializes more reliably.
- The Connector now has an increased window for monitoring network connections.
- The local DFC cache is now being updated correctly.
- Certain IP ranges are no longer incorrectly whitelisted by the Connector.
- Custom IP black/whitelist entries composed of CIDR block and port number combinations are now processed correctly by the Connector.
- The Connector Protection password is no longer logged during the uninstall process.
- Unnecessary TETRA definitions are no longer downloaded when the local definition set is up to date.
- Reduced the likelihood of the Connector generating a new identity on upgrade.
- Scanning of container files (pdf, zip, tar, etc) is now more robust.
- Improved accuracy of parent process reporting.
- Performance of process exclusions has been improved.

18 July 2017

AMP for Endpoints Linux Connector 1.3.1

Bugfixes/Enhancements

- Patched a vulnerability in unrar (CVE-2012-6706)
- Patched a vulnerability in curl (CVE-2017-7468)

11 July 2017

AMP for Endpoints Console 5.4.20170711

New

- The Cisco AMP for Endpoints terms (previously the EULA) have been updated for consistency across the entire Cisco portfolio. The latest version of the Cloud terms can be found at http://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html

Bugfixes/Enhancements

- Changed the Groups list on the Connector download page to be sorted alphabetically.
- (API only) The Executed Malware indication of compromise event includes extra fields like filename and path where available.
- Fixed a bug where policy serial numbers could be incremented incorrectly under certain circumstances.
- Deleted computers are no longer included in the computer count on the Automatic Analysis page.
- Addressed an issue where there could be a discrepancy between the number of licensed computers and the number of computers shown on the Computers page.

6 July 2017

AMP for Endpoints Windows Connector 5.1.9

Bugfixes/Enhancements

- Patched a vulnerability in unrar (CVE-2012-6706)

AMP for Endpoints Mac Connector 1.4.2 (superseded by 1.4.3)

IMPORTANT! AMP for Endpoints Mac Connector 1.3.0 users are strongly advised to upgrade to 1.3.1 then reboot the system before upgrading to 1.4.2. Upgrading directly from 1.3.0 to 1.42 can cause a kernel panic. For more information, please refer to this special advisory.

IMPORTANT! Users running macOS 10.12 (Sierra) should upgrade to 10.12.4 or later. There are compatibility issues that affect system stability which are resolved in macOS 10.12.4.

New

- Rebranded product from Sourcefire FireAMP to Cisco AMP for Endpoints.

  As part of the rebranding, the Connector installation paths have changed to:
  - `/Applications/Cisco AMP`
  - `/Library/Application Support/Cisco/AMP for Endpoints Connector`
  - `/opt/cisco/amp`

  Before upgrading your endpoints to this version, be sure to review any exclusions you have for 3rd party software that is installed alongside AMP for Endpoints.
- Added localization support to the Connector UI for Simplified Chinese, Japanese, and Korean.

Bugfixes/Enhancements

- Fixed a bug in the AMP network kernel extension that can cause a kernel panic.
- Patched a vulnerability in unrar (CVE-2012-6706)
- Fixed a bug where connection to the AMP cloud may fail when SSL inspection is enabled on the network gateway.
- Applied security fixes from 3rd party libraries used by the Connector including OpenSSL, cURL, and xmlsec.
- Fixed a bug where a user-initiated scan could interfere with detections in real-time file operations.

- Strengthened guards against misbehaving UI clients.
- Fixed a bug to ensure that files found to be malicious by the offline engine are scanned using the AMP cloud before generating a detection event.
- Fixed a bug where file paths are included in cloud queries even when the feature is disabled in policy.
- Fixed a bug causing a “too many open files” error after parsing MSXML files.
- Fixed a bug where the AMP daemon may crash after disconnecting from the AMP cloud for an extended amount of time.
- Fixed a bug where user information for some events are missing.
- Fixed a bug causing a UI lockup when performing flash scan.
- Improved the readability of quarantine failure messages.
- Improved resiliency against corrupt ClamAV definition files.
- Removed a dependency on perl in the installer.
- Resolved an issue where the connector could not quarantine malicious resource forks.

20 June 2017

AMP for Endpoints Console 5.4.20170620

New

- Added custom filters and alerting to the Dashboard and Inbox tabs so users can receive email alerts for new compromises.
- Added WannaCry demo data and associated document.

Bugfixes/Enhancements

- Added Windows 7 Japanese and Korean operating systems as options for File Analysis. Windows XP and Windows 7 32-bit operating systems are no longer supported by File Analysis. If you currently have your default image set to one of these on your Business page the default will automatically change to Windows 7 x64.

8 June 2017 Release Notes

AMP for Endpoints Windows Connector 5.1.7

Bugfixes/Enhancements

- Addressed an issue where Connectors installed on Windows SMB servers would cause shared, mapped drives to be inaccessible.

6 June 2017 Release Notes

AMP for Endpoints Console 5.4.20170606

New

- Added support for single sign-on through Active Directory, Okta, and Ping Federate.
- Added a policy option to hide list of exclusions from the AMP for Endpoints Windows Connector UI on versions 5.1.3 and higher.

Bugfixes/Enhancements

- Prevalence now shows data based on a global list of prevalence instead of only your deployment.
- The default values of some policy items have changed when creating new policies:
  - Heartbeat Interval is set to 15 minutes.
  - Send User Name in Events is enabled.
  - Hide File Notifications is enabled.
  - Maximum Scan File Size is set to 50 MB.
  - Maximum Archive Scan File Size is set to 50 MB.
- Command Line Logging policy item is only available when Connector Log Level is set to Debug and Command Line Capture is enabled.
- Default Windows exclusions have been updated when creating a new exclusion set.

1 June 2017 Release Notes

AMP for Endpoints Mac Connector 1.3.1

Bugfixes/Enhancements

- This special release fixes a defect in AMP for Endpoints Mac Connector version 1.3.0 that can cause an unexpected system restart. It is highly recommended that 1.3.0 users upgrade to this version and restart their systems before attempting to upgrade to newer Connector versions. Users currently running 1.2.6 or earlier are encouraged to skip this version and upgrade to newer versions directly.

  Refer to advisory AMP for Endpoints Mac Connector 1.3.0 Defect Can Cause Unexpected System Restart for details.

9 May 2017 Release Notes

AMP for Endpoints Windows Connector 5.1.5

Bugfixes/Enhancements

- Addressed issues where the Connector could lose connection to the cloud when Identity Sync is enabled.
- Addressed an issue where the Connector could be disabled by a user with admin privileges when Connector Protection is enabled.
- Addressed a crash that would occur when attempting to enable debug logging.
- Fixed a crash that could occur during the Connector service shutdown.
- Addressed an issue where a password containing certain special characters was not being parsed correctly when attempting to uninstall the Connector via command line with Connector Protection enabled.
- Addressed a minor issue when multiple quarantine notifications are shown on the endpoint for Korean operating systems.

2 May 2017 Release Notes

AMP for Endpoints Console 5.4.20170502

New

- Added computer description drop-down to Device Trajectory.
- Added Send User Name in Events to Policies for Mac Connector (version 1.3.0 and later)
- Added Send User Name in Events to Policies for Linux Connector (version 1.1.1 and later)

4 April 2017 Release Notes

AMP for Endpoints Console 5.4.20170404

New

- Added process exclusions for AMP for Endpoints Windows Connector 5.1.3 and higher.

Bugfixes/Enhancements

- Added pagination for Significant Compromise Artifacts on Dashboard and Inbox tabs.
- Added the ability to mute Significant Compromise Artifacts on Dashboard and Inbox tabs.
- Added the ability to view details of Significant Compromise Artifacts on Dashboard and Inbox tabs.
- Added file names for SHA-256 artifacts on Dashboard and Inbox tabs.
- Added install_date timestamp to the Computers API so users can see the install dates of Connectors.

AMP for Endpoints Linux Connector 1.3.0

New Features

- Added support for Red Hat Enterprise Linux and CentOS 7.2 and 7.3

Bugfixes/Enhancements

- Fixed a bug where connection to the AMP cloud may fail when SSL inspection is enabled on the network gateway.
- Applied security fixes from 3rd party libraries used by the Connector including OpenSSL, cURL, and xmlsec.
- Fixed a bug where a user-initiated scan could interfere with detections in real-time file operations.
- Strengthened guards against misbehaving UI clients.
- Fixed a bug to ensure that files found to be malicious by the offline engine are scanned using the AMP cloud before generating a detection event.
- Fixed a bug where file paths are included in cloud queries even when the feature is disabled in policy.
- Fixed a bug causing "too many open files" error after parsing MSXML files.
- Fixed a bug where the AMP daemon may crash after disconnecting from the AMP cloud for an extended amount of time.
- Fixed a bug where user information for DFC detection events are missing.
- Improved the readability of quarantine failure messages.
- Improved resiliency against corrupt ClamAV definition files.
- Added abrt crash reports to the Support Tool diagnostic archive.

3 April 2017 Release Notes

AMP for Endpoints Windows Connector 5.1.3

New Features

- The Connector will now register with Windows Security Center when TETRA is enabled via policy and all definitions have completed downloading.

Bugfixes/Enhancements

- Improved system performance when the Connector is installed on systems with VMware Persona Management.
- Addressed an issue where the Connector could cause a BSOD under rare conditions.
- Fixed an issue where the Connector could cause system freezes in some instances.
- Addressed an issue with Endpoint IOC scans consuming high amounts of CPU.
- Fixed an issue where altitudes of older Connectors that are upgraded to 5.1.1 or higher were not modified to be more in line with Microsoft software recommendations.
- The Connector is now able to download TETRA definitions over SSL.
- Fixed an issue on Windows XP where the migration from 'Sourcefire' to 'Cisco' install directories was not working correctly when upgrading from versions prior to 5.1.1.
- Addressed an issue where Cloud Notifications were displayed by default when installing the Connector without an injected policy.
- Added a fix to address a vulnerability in bzip2 (CVE-2016-3189).
- Removed erroneous log lines that appeared when using the Connectivity Test Tool.

7 March 2017 Release Notes

AMP for Endpoints Console 5.4.20170307

Bugfixes/Enhancements

- Added Compromise Event Types to the Dashboard and Inbox tabs.
- Fixed a bug in Applications integration to better align Computer IPs between the AMP for Endpoints Console and Firepower Management Console.
- Authentication server changes will redirect users to a new host when logging in. Any pending password resets may have to be resent.

16 February 2017 Release Notes

AMP for Endpoints Windows Connector 5.1.1

New

- Limited rebranding from Sourcefire FireAMP to Cisco AMP for Endpoints.

IMPORTANT! As part of the rebranding, the Connector default installation path was changed to `C:\Program Files\Cisco\AMP`. Before upgrading your endpoints to this version, be sure to review any exclusions you have for 3rd party software that is installed alongside AMP for Endpoints.

- Added localization support to the Connector UI for Simplified Chinese, Japanese, and Korean.
- Updated the TETRA engine to add support for downloading signature deltas.
- A new Timed Diagnostic Tool option is available in the Cisco AMP for Endpoints Connector Start Menu group.
- A utility to test connectivity from the endpoint to the Cisco cloud is now included in the installation directory.
- Connector binaries are now signed using the Cisco EV code signing certificate.
- The AMP for Endpoints Windows Connector can now be installed on systems that have Secure Boot enabled.

Bugfixes/Enhancements

- Improved stability of the Connector by addressing numerous reported crashes.
- Improved handling of local configuration files to reduce instability due to configuration errors.
- Addressed issue where the Connector network driver could cause a BSOD when Windows Driver Verifier is used against it.
- Modified altitude of the AMP for Endpoints Windows drivers to be more in line with Microsoft software recommendations.
- Addressed an issue where the Connector could become deadlocked.
- Addressed compatibility issues with VMWare View Persona Management and LabLogic Debra.
- Addressed an issue where virtualized systems were not correctly being identified as unique.
- Addressed an issue where the installer would not complete successfully under certain circumstances.
- Addressed an issue where previously downloaded TETRA definitions couldn’t be used after a partial uninstall followed by a re-install.
- Addressed an issue where the Connector would not shut down in a timely fashion while TETRA definitions were being downloaded.

- Fixed an issue where Application Blocking events were not reporting parent process information properly.
- Addressed an issue where log files could grow beyond their maximum size.
- Fixed an issue where the Connector would continue to apply Advanced Custom Detection definitions after they were removed from policy until the Connector was restarted.
- Fixed an issue where HDB Advanced Custom Detection signatures would not be correctly applied when configured to use a wildcard for file size.
- Addressed an issue where the first scan after install would execute without network activity or before TETRA definitions were fully downloaded.
- Addressed an issue where the Connector would negatively impact write performance when installed on machines with solid state drives (SSDs).
- Addressed an issue on Windows XP where the Connector could not acquire the machine's IP address when configured with a static IP address and the "Register this connection's addresses in DNS" option was disabled.

7 December 2016 Release Notes

AMP for Endpoints Console 5.4.20161207

New

- AMP for Endpoints Linux Connector policies now support SOCKS proxies.
- AMP for Endpoints Linux Connector policies now support NTLM authentication via HTTP proxies.
- Added Agentless Cognitive Incidents to show incidents from computers without a Connector in your organization. You must have Cognitive Threat Analytics integration enabled to use this feature.

Bugfixes/Enhancements

- Added filter reset button to Dashboard and Inbox tabs.
- Added IP address and URL artifacts to the Significant Compromise Artifacts on Dashboard and Inbox.
- Various improvements to Dashboard and Inbox behavior based on customer feedback.

5 December 2016 Release Notes

AMP for Endpoints Mac Connector 1.3.0

New

- Added support for Advanced Custom Detections.
- The AMP for Endpoints Mac Connector can capture command line arguments used during execution and send this information to the AMP cloud. This information will be visible in Device Trajectory for administrators with Two-Factor Authentication enabled.
- The Connector will now send cloud queries for LZMA compressed Adobe Flash files, MSO attachments within MS Office 2003 XML files, and Hancom Office files.
- Added scanning of files referenced by startup and launch related plists.
- Upgraded ClamAV engine to 0.99.2.

IMPORTANT! The AMP for Endpoints Mac Connector no longer supports OS X 10.7 as of version 1.3.0.

Bugfixes/Enhancements

- Applied security fixes from third party libraries including OpenSSL, Jansson and Libxml2.
- Fixed a bug that stopped ClamAV from scanning files when disconnected from the cloud.
- Addressed an issue where certain file activity could cause scans to stop prematurely.
- Fixed a bug where files contained inside PDF files were not scanned.
- Fixed a bug where some UDP connections were not monitored.
- Fixed a bug where user information was missing from some events.
- Fixed a bug where some deferred scans were dropped because the deferred scan file was not written to correctly.
- Fixed a bug where the URL reported for some network events were malformed.
- Fixed a bug where Definition Update events were missing from the Events table.
- Fixed a bug where the known viruses count for Definition Update events was incorrect.
- Made automatic ClamAV definition updates more robust.
- Clarify in Execution Blocked events and notifications that no action was taken when the Connector is running in audit mode.
- Removed stale files from ClamAV working directory at daemon start-up.
- Reduced the performance overhead of wildcard exclusions.
- Fixed a bug where a kernel extension could panic if there are active network connections when the daemon is stopping or retrying a failed initialization step.
- Fixed various logging issues.

29 November 2016 Release Notes

AMP for Endpoints Linux Connector 1.2.1

New

- Added support for Red Hat Enterprise Linux and CentOS 6.7 and 6.8.

Bugfixes/Enhancements

- Applied security fixes from 3rd party libraries used by the Connector including OpenSSL, cURL, and Jansson.
- Improved detection capabilities when the Connector does not have connectivity to the AMP cloud.
- Fixed a bug where a custom ClamAV Hash Based Signature (.hdb) containing a wildcard fails to trigger.
- Fixed a bug where some deferred scans were dropped because the deferred scan file is not written to correctly.
- Fixed a bug where files contained inside PDF files were not scanned.
- Fixed a bug where exclusion rules were not treated as case sensitive.
- Removed stale files from ClamAV working directory at daemon start-up.
- Optimized scheduling for ClamAV definition updates.
- Addressed an issue where the Connector would consume high CPU when a local database reached a certain size.
- Addressed issues where the ampcli was not correctly reporting some successful Connector actions.

22 November 2016 Release Notes

AMP for Endpoints Windows Connector 5.0.9

Bugfixes/Enhancements

- Updated curl to version 7.51.0.
- Addressed a vulnerability where Connector Protection could be bypassed during uninstall by entering a specific character in the password field.

15 November 2016 Release Notes

AMP for Endpoints Mac Connector 1.2.6

Bugfixes/Enhancements

- Updated curl version to 7.51.0.
- Addressed an issue where the Connector would consume high CPU when a local database reached a certain size.
- Fixed a bug where the Connector would consume high CPU when some local 3rd party software would periodically touch but not modify files.
- The Connector is now able to successfully quarantine files that have immutable flags set.
- Addressed various issues with scan error reporting.

8 November 2016 Release Notes

AMP for Endpoints Console 5.4.20161108

New

- Dashboard tab has been added to provide a more comprehensive view of compromises and threats to your AMP for Endpoints deployment.
- Inbox tab provides a single view to work on and resolve compromises in your AMP for Endpoints deployment.

Bugfixes/Enhancements

- Added operating system filters to the Low Prevalence Executable page so that files from less widely deployed operating systems wouldn't obscure other low prevalence files.
- Added alert URL to the API for vulnerability data.

AMP for Endpoints Windows Connector 5.0.7

Bugfixes/Enhancements

- Addressed an issue where the AMP for Endpoints Windows Connector could potentially delete files located in the volume root directory (but not files in subfolders) if upgraded from a version of the Connector that was below 4.2.0 and was in a state where the local.xml was corrupted.

  IMPORTANT! This issue affected all previous AMP for Endpoints Windows Connector versions 4.2.0 to 4.4.2 and 5.0.1 to 5.0.5. It is important that you do not use installers from those versions to update Connectors if you previously downloaded them. Please download and use the latest versions 4.4.4 and 5.0.7.

- Improved the ability for the Connector to upgrade/uninstall connectors that are in a crashed state.

IMPORTANT! Upgrading from certain Connector versions will require a reboot. Downloading the new installer or performing an update via policy will provide a list of computers in the selected group or policy that will require a reboot.

AMP for Endpoints Windows Connector 4.4.4

Bugfixes/Enhancements

- Addressed an issue where the AMP for Endpoints Windows Connector could potentially delete files located in the volume root directory (but not files in subfolders) if upgraded from a version of the Connector that was below 4.2.0 and was in a state where the local.xml was corrupted.

  IMPORTANT! This issue affected all previous AMP for Endpoints Windows Connector versions 4.2.0 to 4.4.2 and 5.0.1 to 5.0.5. It is important that you do not use installers from those versions to update Connectors if you previously downloaded them. Please download and use the latest versions 4.4.4 and 5.0.7.

- Improved the ability for the Connector to upgrade/uninstall connectors that are in a crashed state.

IMPORTANT! Upgrading from certain Connector versions will require a reboot. Downloading the new installer or performing an update via policy will provide a list of computers in the selected group or policy that will require a reboot.

25 October 2016 Release Notes

AMP for Endpoints Windows Connector 5.0.5 (superseded by 5.0.7)

Bugfixes/Enhancements

- Addressed an issue where the Connector could show up as a new computer in the AMP for Endpoints Console after upgrading to version 5.0.X from version 4.4.2 or below.
- Fixed an issue where the 5.0.X Connector was failing to communicate with the cloud when configured to use a proxy with NTLM authentication.
- Fixed an issue where Connector events related to installing and upgrading were sometimes not sent to the cloud.

IMPORTANT! Upgrading from 5.0.x to 5.0.5 does not require a reboot. Upgrading from all other previous versions **will require a reboot**.

17 October 2016 Release Notes

AMP for Endpoints Windows Connector 5.0.3 (superseded by 5.0.7)

Bugfixes/Enhancements

- Addressed an issue with AMP for Endpoints Windows Connector v5.0.1 where the uninstaller was not honoring command line arguments.

IMPORTANT! Upgrading from 5.0.1 to 5.0.3 does not require a reboot. Upgrading from all other previous versions **will require a reboot**.

6 October 2016 Release Notes

AMP for Endpoints Console 5.4.20161006

New

- Added policy options for AMP for Endpoints Windows Connector 5.0 command line capture.

Bugfixes/Enhancements

- Fixed a bug where pagination on the Audit Log for a single computer was broken.
- Fixed an issue where attempting to view matching endpoint IOCs from an IOC scan caused an error.

AMP for Endpoints Windows Connector 5.0.1 (superseded by 5.0.7)

New

- The AMP for Endpoints Windows Connector now uses CiscoSSL to communicate with the AMP Cloud. The Connector will use two new servers to perform cloud lookups as part of this change. See the AMP for Endpoints User Guide for new firewall exceptions.

IMPORTANT! AMP for Endpoints Windows Connector 5.0.1 only supports cloud lookups on TCP port 443.

- The AMP for Endpoints Windows Connector can capture command line arguments used during execution and send this information to the AMP cloud. This information will be visible in Device Trajectory for administrator users with Two-Factor Authentication enabled.
- ClamAV upgraded to 0.99.2.

Bugfixes/Enhancements

- Fixed an issue where TETRA could incorrectly flag files as malicious.
- Fixed an issue where TETRA was not handling the detection of malicious archive files properly in certain situations.
- Fixed a rare issue where the Connector would cause high CPU usage due to MTU and policy size.
- Addressed an issue where the Connector process was able to be stopped via debugger access.
- Improved validation of new policies to ensure continued connectivity with the AMP cloud.
- Users are now able to configure which path to store temporary files during the installation process through a command line switch.

- Improved the uninstall process to better handle scenarios where the Connector is in a bad state prior to uninstalling.
- Improved overall stability of the Connector.
- Addressed a minor issue where the Connector would report a successful custom scan for invalid paths.
- Fixed an issue where partial connectivity to the AMP cloud would cause installs to hang indefinitely.
- Improved error reporting.

IMPORTANT! Upgrading to AMP for Endpoints Windows Connector 5.0.1 from all previous Connector versions will require a reboot.

29 September 2016 Release Notes

AMP for Endpoints Mac Connector 1.2.5

Bugfixes/Enhancements

- Addressed a compatibility issue with AMP for Endpoints Mac Connector 1.2.4 and OS X 10.12. All users who are running Connector version 1.2.4 should upgrade to 1.2.5.

27 September 2016 Release Notes

AMP for Endpoints Linux Connector v1.2.0

New

- Added support for Advanced Custom Detections.
- The AMP for Endpoints Linux Connector can capture command line arguments used during execution and send this information to the Cisco cloud. This information will be visible in Device Trajectory for administrator users with Two-Factor Authentication enabled.
- ClamAV upgraded to 0.99.2.
- The Connector will now send cloud queries for LZMA compressed Adobe Flash files, MSO attachments within MS Office 2003 XML files, and Hancom Office files.

Bugfixes/Enhancements

- Fixed a bug that caused some network detection events not to be reported to the cloud correctly.
- Fixed a bug that caused ClamAV not to scan files when it was disconnected from the cloud.
- Addressed an issue where ClamAV definitions could get into a bad state.
- Made automatic ClamAV definition updates more robust.
- Addressed an issue where under certain circumstances a requested file could not be uploaded to the File Repository.
- Fixed a bug where some retrospective operations could fail because of missing data.
- Files installed from a trusted and signed RPM package will not be quarantined.
- Reduced the performance overhead of wildcard exclusions.
- Fixed a bug that could cause DNS resolution errors after a paused virtual machine was resumed.
- Fixed issues with Connector logging.

Special Advisory

Important note for RHEL and CentOS 6.0-6.5 users

Confirm the installed version of procps is 3.2.8-30 or newer prior to installing this update. Older versions of procps are not compatible and users are advised to update to the latest version. Refer to the following Red Hat advisories for details:

https://rhn.redhat.com/errata/RHBA-2014-1595.html

https://rhn.redhat.com/errata/RHBA-2015-1407.html

https://rhn.redhat.com/errata/RHBA-2015-1812.html

https://rhn.redhat.com/errata/RHBA-2015-2643.html

https://rhn.redhat.com/errata/RHBA-2016-0904.html

20 September 2016 Release Notes

AMP for Endpoints Console v5.4.20160920

Bugfixes/Enhancements

- Added a date filter to the filters on the Events page. You can choose to view events from the past day, week, or all events.
- Demo data computers now have MAC addresses available to API users.

8 September 2016 Release Notes

AMP for Endpoints Mac Connector v1.2.4.431 (superseded by 1.2.5)

New

- Added Support for Mac OS X 10.12

Bugfixes/Enhancements

- Fixed an issue where you could not fetch a file from a computer after it was deleted even if other copies of the same file existed on the computer.
- Addressed an issue where the Connector would only perform a Retrospective Quarantine on the first instance of a file on the computer.
- Fixed a bug where scans in progress when the computer was rebooted did not appear to complete in the Console.

7 September 2016 Release Notes

AMP for Endpoints Console v5.4.20160907

New

- Added Cognitive Threat Analytics examples to Demo Data.

23 August 2016 Release Notes

AMP for Endpoints Console v5.4.20160823

Bugfixes/Enhancements

- Fixed a bug where Audit Log filters were not being applied properly.

9 August 2016 Release Notes

AMP for Endpoints Console v5.4

Bugfixes/Enhancements

- Rebranded FireAMP Console to AMP for Endpoints.

12 July 2016 Release Notes

AMP for Endpoints Mac Connector v1.2.2.407

Bugfixes/Enhancements

- Fixed an issue where outdated ClamAV definitions were still being loaded by the Connector in some instances. This could potentially cause an increase in false-positive detections.

5 July 2016 Release Notes

AMP for Endpoints Console v5.3.20160706

New

- Added an API call to retrieve all AMP for Endpoints Connector GUIDs from a specified group.
- Users can now choose to receive Console Announcements via email.
- Administrators can now allow unprivileged users to fetch files from the groups they have permission to access.

8 June 2016 Release Notes

AMP for Endpoints Console v5.3.20160607

New

- AMP for Endpoints is now integrated with Cisco Cognitive Threat Analytics. A user with a supported web proxy can use this integration for increased visibility and efficacy.

Bugfixes/Enhancements

- Added new exclusions to AMP for Endpoints Windows Connector default policies for Microsoft Windows Defender.

26 May 2016 Release Notes

AMP for Endpoints Console v5.3.20160526

New

- The AMP for Endpoints API now allows you to make changes to your business. API users can move computers, assign policies to groups, and make modifications to Application Blocking and Simple Custom Detection lists.
- Added an API Credentials page to simplify 3rd party application management.

Bugfixes/Enhancements

- Added links to Weekly Reports sections. These links will take you to the appropriate section of the AMP for Endpoints Console filtered to the same view as the report metric.
- The SHA-256 of archive files are now displayed when a detection is triggered by a file contained within the archive.
- Clarified detection events when a Connector is in a group with a policy that uses Audit Mode.

19 May 2016 Release Notes

AMP for Endpoints Windows Connector 4.4.2 (superseded by 4.4.4)

Bugfixes/Enhancements

- Patched ClamAV engine to address potential vulnerabilities when handling certain archive file types (CVE-2016-1371, CVE-2016-1372).
- Fixed an issue where the Connector was not sending information about the current user for certain events.
- Addressed a bug where TETRA definition downloads did not appear to complete successfully even though they did.
- Fixed a problem where the Connector was not reporting the parent file type correctly in some cases.

AMP for Endpoints Mac Connector v1.2.2.382

Bugfixes/Enhancements

- Patched ClamAV engine to address potential vulnerabilities when handling certain archive file types (CVE-2016-1371, CVE-2016-1372).
- Modified the Connector installer to prevent downgrades when running the installer locally.
- Added more diagnostic information collected by the Support Tool.
- Improved performance when using Application Blocking lists on Mac OS X 10.8 and 10.9.
- Improved handling of nested archive files.
- Fixed an issue where the Connector was not sending information about the current user for certain events.
- Fixed an issue where the Connector wasn't cleaning up its child processes.
- The Connector will now try to connect directly to the Cisco Cloud if it can't contact the proxy server configured in Policy.

AMP for Endpoints Linux Connector v1.1.0.277

Bugfixes/Enhancements

- Patched ClamAV engine to address potential vulnerabilities when handling certain archive file types (CVE-2016-1371, CVE-2016-1372).
- Fixed an issue where the Connector was not sending information about the current user for certain events.
- Fixed an issue where retrospective restore operations would sometimes fail.

- Improved handling of nested archive files.
- The Connector will now try to connect directly to the Cisco Cloud if it can't contact the proxy server configured in Policy.
- Addressed an issue where the CLI history page couldn't display very long file paths properly.
- Improved logging to aid in debugging Connector issues.

26 April 2016 Release Notes

AMP for Endpoints Console v5.3.20160426

New

- VirusTotal integration on the right-click context menu.
- Added information about reboot requirements to Product Update section of Policies and to the Download Connector page.

14 April 2016 Release Notes

AMP for Endpoints Windows Connector 4.4.1 (superseded by 4.4.4)

Bugfixes/Enhancements

- Addressed an issue where the TETRA engine was generating false-positive detections. Customers who experienced this issue have already been notified by Cisco Support.
- Improved error handling when upgrading from previous versions of the AMP for Endpoints Windows Connector.

IMPORTANT! This upgrade does not require a reboot when upgrading from version 4.3.1 or 4.4.0 of the AMP for Endpoints Windows Connector.

7 April 2016 Release Notes

AMP for Endpoints Linux Connector v1.0.2.261

New

- The AMP for Endpoints Linux Connector now supports Remote File Fetch.
- Added RAR archive scanning.

Bugfixes/Enhancements

- Reduced cloud communication overhead by optimizing local caches.
- Improved overall stability and memory usage.
- Improved logging to help with debugging Connector issues.
- Resolved an issue where the Connector updater fails when SELinux is enabled.
- Fixed a compatibility issue with OpenVPN.
- Fixed various problems with handling user-created exclusions.
- Fixed a bug where the Connector reported extraneous file creation and execution events.
- Addressed an issue where ClamAV definitions would sometimes be placed in the incorrect path.
- Improved the ability to handle malicious forking executable files.
- Addressed issues with Connectors installed on virtual machines that are paused then resumed.
- Fixed a bug where the local restore operation could be initiated by an unprivileged user.

IMPORTANT! Because of an issue with the updater in version 1.0.0 of the AMP for Endpoints Linux Connector, users performing upgrades through policy settings may see one or more Update Failed events. This is expected and the Connector will automatically schedule another attempt after each failure. The upgrade process should complete successfully within 24 hours. Manual upgrades through rpm or yum are not affected.

31 March 2016 Release Notes

AMP for Endpoints Windows Connector 4.4.0 (superseded by 4.4.4)

New

- The endpoint IOC scanner now supports the ability to only catalog changes in the filesystem, allowing IOC scans to complete faster after the first full catalog has been completed.
- AMP for Endpoints Windows no longer requires Windows administrator credentials for scheduled scans.

Bugfixes/Enhancements

- Improved Connector stability, particularly with regards to shutting down the AMP for Endpoints service cleanly.
- Improved Connector reliability during installation and upgrades.
- The Connector now dynamically honors file scan size limits when changed in policy. Previously the Connector service would have to be stopped and restarted.
- Fixed various issues with exclusion handling.

- Policy update events in the AMP for Endpoints console now accurately reflect the serial number of the acquired policy.
- Improved Connector error reporting to assist in troubleshooting.
- Improved handling of archive files.
- Fixed an issue where upgrades performed by installing the new Connector version over a previous version would not honor non-driver related command line switch options.

IMPORTANT! This upgrade does not require a reboot when upgrading from version 4.3.1.10163 of the AMP for Endpoints Windows Connector.

24 March 2016 Release Notes

AMP for Endpoints Mac Connector v1.2.0.368

New

- The AMP for Endpoints Mac Connector now uses CiscoSSL to communicate with the AMP Cloud. The Connector will use two new servers to perform cloud lookups as part of this change. See the AMP for Endpoints User Guide for new firewall exceptions.

  IMPORTANT! AMP for Endpoints Mac Connector 1.2.0 only supports cloud lookups on TCP port 443.

- A command line interface has been added to the AMP for Endpoints Mac Connector. This can be used to initiate scans, sync policies, show the Connector history, and more.

Bugfixes/Enhancements

- ClamAV updated to version 0.98.7.
- Improved overall Connector stability and efficiency.
- Addressed issue where ClamAV would download definitions more often then necessary.
- Resolved issue where Connector sent extraneous file execute events.
- Addressed various memory usage issues.
- Improved DFC engine to robustly handle network events.
- Improved file move event detection data for better representation in Device Trajectory.
- Fixed issue where the connector was not clearing the file scan queue in some cases.
- Improved various UI messages and error notifications.
- Improved messaging for events displayed in the management console.
- Improved error messaging when attempting a custom scan for an invalid path.
- Improved Connector upgrade functionality and console notifications.
- Connector updated to dynamically honor file scan size limits on policy change.

- Fixed various issues with exclusion handling.
- Improved handling of archive files.
- Improved ability of the connector to handle malicious forking executable files.
- Improved Connector compatibility for OS X 10.10 and above.
- Addressed issue where upgrading OS X with the Connector installed would sometimes freeze the system.
- Improved Connector performance when installing from read-only media (e.g. DVDs).
- Addressed issue where cache TTLs were not expiring as expected.
- Changed Support Package creation process improving efficiency and flexibility.
- Added ability to specify custom output path for Support Package using “-o” option.

22 March 2016 Release Notes

AMP for Endpoints Console v5.3.20160322

Bugfixes/Enhancements

- Added support for Hangul Word Processor files.These files will now appear in File and Device Trajectory and can be submitted for File Analysis.
- In rare situations where a File Analysis submission keeps failing, AMP for Endpoints would continue trying to submit the file indefinitely. A limit has been added so that it will stop trying to submit the file after seven days.

25 February 2016 Release Notes

AMP for Endpoints Console v5.3.20160226

New

- Weekly reports added with a new interface under Analysis > Reports. Previous reports are still accessible through the old Reports link but you will not be able to create any new reports through that interface. Previously created scheduled reports will continue to run.

22 February 2016 Release Notes

AMP for Endpoints Mac Connector v1.0.8.352

Bugfixes / Enhancements

- Increased local cloud cache size to reduce Connector network usage.
- Improved performance of the local scanning engine.
- Updated exclusions for the version of mail.app included with Mac OS X 10.11.

10 February 2016 Release Notes

AMP for Endpoints Console v5.3.20160210

Bugfixes / Enhancements

- Added the ability to limit the number of Cisco AMP Threat Grid daily submissions consumed by File Analysis and Automatic Analysis. The number of remaining submissions for the day is also displayed.
- You can now select which VM operating system image to use for Cisco AMP Threat Grid file analysis.
- Limited the number of CVE IDs displayed per application on the Vulnerabilities page to the ten most recent and severe.
- Changed the hostnames for the Cisco cloud servers that are used by the Connectors. The cloud servers now use static IP addresses as well to improve customer ability to allow firewall exceptions for endpoint Connector communication. This rollout will be gradually staged among AMP for Endpoints users and a tool will be in the AMP for Endpoints console to help migrate your existing policies to use the new static IP addresses when it becomes available to you.

5 February 2016 Release Notes

AMP for Endpoints Windows Connector 4.3.1 (superseded by 4.4.4)

Bugfixes / Enhancements

- Addressed an issue where AMP for Endpoints Windows Connector v4.3.0.10148 had an issue with quarantining certain malicious files that were digitally signed even though they were detected. Windows Connector v4.3.0.10148 has been removed from the console so you should upgrade as soon as possible. Upgrading from v4.3.0.10148 to v4.3.1.10163 does not require a reboot.
- Addressed an issue where IOC Flash Scans were not correctly cleaning up files from previous scans.

IMPORTANT! This upgrade does not require a reboot when upgrading from version 4.3.0.10148 of the AMP for Endpoints Windows Connector.

15 December 2015 Release Notes

AMP for Endpoints Console v5.3.20151215

New

- Users can now specify their timezone so dates and times will be displayed in the chosen timezone throughout the Console.
- Clicking a date entry anywhere will show a pop-up menu with additional options.
- Added global search to the menu bar throughout the Console. This is the same search that can be accessed via Analysis > Search.
- Added view changes links that will take you to a filtered view of the Audit Log.
- Added filters to the Audit Log page.

Bugfixes / Enhancements

- Redesigned the Audit Log page for usability.
- Cisco AMP Threat Grid API query limits for File Analysis are now shown on the Business page.
- Moved version number to Help dialog.

AMP for Endpoints Windows Connector 4.3.0 (superseded by 4.4.4)

New

- Starting with upgrades from version 4.3.0 to future versions, the AMP for Endpoints Windows Connector no longer requires a reboot after every update.

  IMPORTANT! Updates that include major functionality changes or bugfixes may still require a reboot.

- Added support for Windows 10.

Bugfixes / Updates

- Added cloud lookup support for XML, PPT, and DOC files.
- Connector force reboot timer is now configurable via policy to be 2, 10, or 30 minutes.
- TETRA definitions can now be downloaded when the Connector is configured to use a proxy server.
- You can now stop the Connector service via the command line when Connector Protection is enabled.
- Made improvements to the installer for preserving previous command line options.
- Various stability improvements and bugfixes.

24 November 2015 Release Notes

AMP for Endpoints Console v5.2.20151124

Bugfixes / Enhancements

- Fixed a bug that caused policy updates to fail in certain situations.
- Added Event Type filters for product updates.
- API now includes file path and name when querying trajectory data.
- MAC addresses for computers are now included in CSV export and API query results.
- Fixed a bug that caused the incorrect file type to be displayed in trajectory data.

15 October 2015 Release Notes

AMP for Endpoints Console v5.2.20151015

New

- An Application Programming Interface (API) is now available, allowing users to access the data and events in their account without logging into the Console.

Bugfixes / Enhancements

- Added option to select ClamAV content update frequency in AMP for Endpoints Mac Connector policy.

AMP for Endpoints Mac Connector v1.0.7.330

Bugfixes / Enhancements

- Added support for OS X 10.11
- Addressed issues causing Time Machine backups to take a long time over AFP.
- Fixed an issue where the Connector would block applications while in Audit mode.
- Optimized Flash Scans for faster performance.
- Various bug fixes.

30 September 2015 Release Notes

AMP for Endpoints Linux Connector v1.0.0.184

New

- New Connector supports CentOS 6.4/6.5/6.6 and Red Hat Enterprise Linux 6.5/6.6
- Includes SHA-256 matching, ClamAV offline engine, and device flow correlation features.
- Supports current lists including Simple Custom Detections, Application Control, Network, and Exclusions.
- New AMP for Endpoints Linux policies can be added to existing AMP for Endpoints Groups.

21 September 2015 Release Notes

AMP for Endpoints Windows Connector 4.1.4

AMP for Endpoints Windows Connector 4.2.1 (superseded by 4.4.4)

Bugfixes / Enhancements

- Addressed an issue where the Connector could become disconnected from the cloud. The computer may appear as a newly installed Connector in the default group if this problem occurs. AMP for Endpoints Windows versions 4.1.0.10054, 4.1.1.10073, and 4.2.0.10084 are affected.

14 September 2015 Release Notes

AMP for Endpoints Console v5.2.20150914

Bugfixes / Enhancements

- Several UI improvements to enhance usability and consistency.
- Various bugfixes and improvements.

13 August 2015 Release Notes

AMP for Endpoints Console v5.2.20150813

Bugfixes / Enhancements

- AMP Threatgrid score for files submitted to File Analysis is now displayed.
- New malware samples added to Demo Data.
- Various bugfixes and improvements.

21 July 2015 Release Notes

AMP for Endpoints Console v5.2.20150721

New

- Added an option to subscribe to individual event alert emails.
- You can now export Vulnerable Programs data to a CSV file.
- Added the ability to search for computers by Connector GUID.
- Added new Indication of Compromise event called Suspicious Cscript Launch to flag when Internet Explorer launches a command shell that in turn launched the Microsoft Script Host (cscpript.exe).

Bugfixes / Enhancements

- Improved Groups page interface, including creating and editing groups.

16 July 2015 Release Notes

AMP for Endpoints Windows Connector 4.2.0 (superseded by 4.4.4)

Bugfixes / EnhancementsBugfixes / Enhancements

- Enhanced scope of Endpoint IOC flash scan indexing to provide increased coverage. Please refer to the Cisco Endpoint IOC Attributes document for more information.
- Improved performance during the Endpoint IOC collection phase to reduce collection time.
- Addressed issues where the Connector install would occasionally fail.
- Improved overall Connector stability.
- Various bugfixes.

16 June 2015 Release Notes

AMP for Endpoints Console v5.2.20150616

Bugfixes / Enhancements

- Improved User Permissions page interface.
- Improved Outbreak Control lists interface.
- Added the ability to easily revert back to default AMP Threat Grid API key.

28 May 2015 Release Notes

AMP for Endpoints Windows Connector v4.1.1.10073

Bugfixes / Enhancements

- Improved efficiency of the exclusion engine when handling wildcard exclusions.
- Fixed a bug that would cause the Connector crash reporting tool to fail.
- Fixed an issue where the Connector would crash if left in debug mode for an extended period of time.
- Fixed a bug where the Connector was unable to retrieve the local computer's fully qualified domain name (FQDN) properly on certain systems.

12 May 2015 Release Notes

AMP for Endpoints Console v5.2.20150512

New

- Added the ability for administrators to assign unprivileged users access to view groups, edit policies, and create and edit outbreak control lists.

Bugfixes / Enhancements

- Fixed an issue so that all user actions on Advanced Custom Detection lists are now recorded in the Audit Log.

16 April 2015 Release Notes

AMP for Endpoints Mac Connector v1.0.6.292

New

- Added the ability to specify the output path of Support Packages with a command line parameter.

Bugfixes / Enhancements

- Performance improvements in the file scanning engine for more efficient calculation of file hashes and ClamAV scanning.
- Added additional monitoring of startup plist files for more IOC detection capabilities.

- Eliminated incorrect notifications when attempting a manual policy sync through the endpoint UI.
- Resolved issue where erroneous log messages appeared at system startup.
- Less ambiguous endpoint notifications by displaying “Off-line” when system is not connected to a network or the interface is disabled and “Service Unavailable” if there are problems connecting to the cloud.

7 April 2015 Release Notes

AMP for Endpoints Console v5.1.2015040718

New

- Vulnerabilities page shows executable files with known vulnerabilities observed by your AMP for Endpoints Windows Connectors.
- Added a configuration item in Policies to enable or disable automatic crash dump log file uploads to the AMP for Endpoints cloud.
- You can now view all applications on devices with the AMP for Endpoints Android Connector installed.
- Added new Indication of Compromise event called Suspicious Download to flag executable files downloaded from numeric public IP addresses over a non-standard port.

Bugfixes / Enhancements

- Fixed an issue that cause files older than 30 days not to be displayed on the File Analysis page.
- Fixed an issue that caused some data not to be visible in Device Trajectory when the page was accessed from search results.
- Added IP addresses to CSV exports from the Computers page.

26 March 2015 Release Notes

AMP for Endpoints Console v5.1.2015032618

Bugfixes / Enhancements

- AMP for Endpoints Mac Connector policies updated to improve cloud query efficiency.

12 March 2015 Release Notes

AMP for Endpoints Windows Connector v4.1.0.10054

New

- ClamAV engine updated to version 0.98.5
- TETRA engine updated to version 3.0.0.71
- Connector process protection added for Windows Vista, Windows 7, Windows Server 2003, and Windows Server 2008.

Bugfixes / Enhancements

- Added enforcement of size limits for Connector log files to a maximum of 10 files, each up to 50MB in size at any given time.
- Advanced Custom Signatures can now be dynamically applied without restarting the Connector.
- Improved error reporting during policy update failures.
- Connector uninstall events are now properly reported from behind a proxy.
- Connector is now able to perform Identity Synchronization from behind a proxy.
- Fixed a bug where the Connector could crash when scanning certain file types.
- Fixed a vulnerability where an unprivileged user could cause the Connector to crash through the UI.
- Fixed a bug where using the Microsoft Application Verifier tool could cause the Connector to crash.

4 March 2015 Release Notes

AMP for Endpoints Console v5.1.20150304

New

- Low Prevalence Executables can be configured to automatically be submitted for File Analysis.
- Export computer details to a CSV file from the Computers page.
- Announcements will alert the user of new releases or upcoming system maintenance.
- Added support for entering a custom Cisco AMP Threat Grid API key.

Bugfixes / Enhancements

- Added the ability to bulk delete computers from the Computers page.
- Improved bulk move operations on the Computers page.
- Fixed a bug where incorrect files were being downloaded when the user tried to download PCAP files from File Analysis.
- File Analysis search is now performed either in the Your Files or Global Files context.
- Removed the Connector 3.0 ClamAV Compatibility Mode policy setting because AMP for Endpoints Windows Connector 3.0 is deprecated and no longer supported, making this option obsolete.

AMP for Endpoints Mac Connector v1.0.5.279

New

- AMP for Endpoints Mac Connector officially certified on OS X 10.10.

Bugfixes / Enhancements

- Addressed compatibility issue with OS X mail.app where malicious emails are continually downloaded and quarantined by the AMP for Endpoints Mac Connector. The Connector now detects and notifies that malicious emails are present but does not quarantine malicious .emlx files created by mail.app. It is left to the administrator to remove the malicious email from the server manually. If mail.app is configured to automatically download attachments and those are determined to be malicious, the Connector will continue to quarantine those attachments.

  IMPORTANT! This fix only affects OS X mail.app. Other email applications may behave differently.

- Resolved a rare issue where the Connector is unable to sync policies for some period of time.

- Addressed a performance issue where users experienced high CPU usage after waking the computer from sleep or performing a reboot.
- Fixed high CPU usage issues on OS X 10.10 due to changes in Spotlight.
- Eliminated a race condition where kernel extensions were unable to successfully unload on shutdown or reboot.
- Improved Connector validation of user-created exclusions.

18 February 2015 Release Notes

AMP for Endpoints Console v5.1.20150218

Bugfixes / Enhancements

- Upgraded AMP for Endpoints Mac Connector protocol version to improve compatibility and reliability. This update is required to ensure future connectivity between the Cisco cloud and AMP for Endpoints Mac Connectors. All AMP for Endpoints Mac Connector policies will be updated to enable this change.
- Fixed a bug to address compatibility of the OpenIOC format with the AMP for Endpoints Endpoint IOC engine. Users experiencing false positives with Endpoint IOCs should re-upload them.

5 February 2015 Release Notes

AMP for Endpoints Console v5.1.20150204

Bugfixes / Enhancements

- Fix to allow users to search File Analysis results by SHA-256 or file name.

29 January 2015 Release Notes

AMP for Endpoints Console v5.1.20150129

New

- File Analysis now fully integrated with Cisco AMP Threat Grid.
- The Computers page can now be filtered by the last time an endpoint connected to the Cloud.
- Added a new UI feature to view all dates and timestamps in various formats by right-clicking the date to open a context menu.

Bugfixes / Enhancements

- Performance improvements to Device Trajectory load times.

11 December 2014 Release Notes

AMP for Endpoints Console v5.1.20141211

New

- Added the ability to create administrator and unprivileged user accounts in the AMP for Endpoints Console.

Bugfixes / Enhancements

- Fixed cross-site scripting issues on several pages.
- Various minor bugfixes and enhancements in page appearance.

2 December 2014 Release Notes

AMP for Endpoints Mac Connector v1.0.4.259

Bugfixes / Enhancements

- Fix for a WebDAV kernel panic issue.
- Fix for a race condition that would cause policy update failures.
- Significant performance improvement from file event queue optimization.
- Compatibility update for OS X 10.10 Yosemite related to the metadata indexer.
- Cleanup of erroneous Connector syslog messages.

8 November 2014 Release Notes

AMP for Endpoints Console v5.0.2014

Bugfixes / Enhancements

- Fixes on various list pages and reports for when users who created the lists or reports have been deleted. The creator of these lists will now show as unknown.
- Fixed a query that occasionally impacted moving groups.
- Allow provisioning to supply multiple email addresses.
- Fixed auto refresh on the Dashboard Overview tab.

1 November 2014 Release Notes

AMP for Endpoints Console v5.0.20141031

Bugfixes / Enhancements

- Various bugfixes for support cases.

28 October 2014 Release Notes

AMP for Endpoints Console v5.0.20141028

New

- Added Group Filter to Dashboard, Threat Root Cause, and Deployment Summary pages that allow the view to be filtered based on selected Groups.

Bugfixes / Enhancements

- Redesigned Computers page with new computer view. You can now filter the view and move multiple computers to new Groups.
- Redesigned Users page with new layout. You can now search user accounts by name and email address and quickly access your own account.
- Installed Endpoint IOCs page now allows you to filter view based on the Endpoint IOC state and also activate, deactivate, and delete Endpoint IOCs in bulk.

23 October 2014 Release Notes

AMP for Endpoints Windows Connector v4.0.2.10018

New

- Expanded official support for Endpoint IOC scans to include all Windows platforms supported by the AMP for Endpoints Windows Connector.

Bugfixes / Enhancements

- Various bugfixes to improve the IOC Scanner engine.

16 October 2014 Release Notes

AMP for Endpoints Mac Connector v1.0.3.228

New

- Added Event History, Policy View, Local Scanning, and Headless Mode to the user interface.

IMPORTANT! If the user interface is not visible on a Connector after the update, check the Start Client User Interface setting in your policy.

IMPORTANT! Connectors upgrading from 1.0.2 will not show all previous events in the History Pane.

Bugfixes / Enhancements

- Added notifications for Device Flow Correlation, definition updates, Cloud Recall, and product updates.
- Updated ClamAV library to support scanning raw DMG files.
- Performance improvements.
- Various fixes for support cases.

8 October 2014 Release Notes

AMP for Endpoints Console v5.0.20141008

Bugfixes / Enhancements

- Enhanced Endpoint IOC documentation regarding time expectations for re-cataloging of attributes.
- Better identification of Computers page for running scans for individual computers.
- Removed Send Files for Analysis policy item and turned this setting off for all AMP for Endpoints Connectors.
- Removed On Copy Mode and On Move Mode policy items and made these settings Passive for all AMP for Endpoints Connectors.
- Removed Unseen Cache TTL policy item as this was not used by the AMP for Endpoints Connector.
- Various fixes for support cases.

7 October 2014 Release Notes

AMP for Endpoints Windows Connector v4.0.1.10011

Bugfixes / Enhancements

- Fixed a bug caused by the accumulation of archived ClamAV logs that could result in computers running out of disk space. Archived ClamAV logs are now deleted hourly.

AMP for Endpoints Windows Connector v3.1.15.9681

Bugfixes / Enhancements

- Fixed a bug caused by the accumulation of archived ClamAV logs that could result in computers running out of disk space. Archived ClamAV logs are now deleted hourly.

25 September 2014 Release Notes

AMP for Endpoints Console v5.0.20140925

New

- Endpoint Indication of Compromise (IOC) feature added.

Bugfixes / Enhancements

- Minor changes to First Use Wizard.
- Various fixes for support cases.

AMP for Endpoints Windows Connector v4.0.0

New

- Added Endpoint Indication of Compromise (IOC) scanner.

IMPORTANT! This feature is currently only supported on Windows XP SP3 and Windows 7.

Bugfixes / Enhancements

- Fix to address high CPU usage under certain scenarios.

18 August 2014 Release Notes

AMP for Endpoints Mac Connector v1.0.2

- Various bug fixes.
- Added Remote File Fetch functionality.

IMPORTANT! A bug in version 1.0.1 of the AMP for Endpoints Mac Connector prevents upgrading automatically through policy. To upgrade to version 1.0.2 you will have to download the installer and run it manually.

24 July 2014 Release Notes

AMP for Endpoints Console v4.5.20140724

New

- Completely redesigned File Analysis page for better clarity and consistency within the AMP for Endpoints Console.
- Redesigned and consolidated the Connector download page.
- Added Maximum Scan File Size and Maximum Archive Scan File Size items to AMP for Endpoints Windows Connector policies.

Bug Fixes/Enhancements

- Minor fixes to online help.
- Addressed an issue where two-step verification was not syncing correctly with the Google Authenticator app.
- Fixed an issue where event filters containing special characters could cause a javascript exception.

26 June 2014 Release Notes

AMP for Endpoints Console v4.5.20140623

New

- AMP for Endpoints Windows Connector installers are now compliant with Authenticode Signature Verification changes (https://technet.microsoft.com/en-us/library/security/2915720.aspx).

Bug Fixes/Enhancements

- SHA-256 values on File Repository page are now color-coded based on disposition.
- Removed Verbose Notifications policy item from AMP for Endpoints Mac Connector policies.
- Warning added about uploading files greater than 20MB to File Analysis.

15 May 2014 Release Notes

Connector 3.1.10

Bugfixes / Enhancements

- Update to TETRA license information. All Connectors with TETRA enabled should upgrade to this version.
- Fixed an issue when saving Microsoft Excel spreadsheets to a network share.

8 May 2014 Release Notes

AMP for Endpoints Console 4.5.20140508

New

- Google Authenticator app now shows AMP for Endpoints Console as part of the account information.
- Search results now include files that were remotely fetched.
- Outbreak control search results now redirect to the correct list.
- Notification emails are now sent to users when a file is fetched.
- Events page now shows remote file fetch events.
- File fetch content menu updated to indicate status of file.

Bugfixes / Enhancements

- Deployment URL has been added to Connector email deployment page to allow users to send URL through their own mail accounts.
- Android devices will no longer report as Windows XP under operating system.
- Email addresses with multiple extensions (ie. yahoo.co.uk) will now work correctly.
- Users can now specify a different email address to receive notifications.

AMP for Endpoints Mac Connector v1.0.1

Bugfixes / Enhancements

- Over 40 defects related to scanning and caching of files, console events, and cloud functionality addressed.
- Application blocking lists are now honored correctly.
- Fixed an issue that interfered with Time Machine backups over a network.
- Addressed a problem where CPU usage would climb to 100% during an idle state.

10 April 2014 Release Notes

AMP for Endpoints Console v4.5.20140410

New

- Ability to request individual files from computers running version 3.1.9 of the AMP for Endpoints Windows Connector.

Bugfixes / Enhancements

- First Use wizard can now be accessed after initial setup from the Management > Quick Start menu item.
- Enhancements to Search page for better quality and clarity of results.
- Beta tag has been removed from the Search feature.
- Updated documentation to include EU-specific AMP for Endpoints servers.
- Minor fixes for Two-Step Verification.
- Redesigned Business page.

Connector 3.1.9

New

- Allows AMP for Endpoints administrators to use Remote File Fetch to request individual files from computers.
- Added support for installation on Windows Server 2012.

Bugfixes / Enhancements

- Fixed an issue with slowness when saving Microsoft Excel spreadsheets to network shares.
- Added support for CNAMEs on initial lookup of AMP for Endpoints servers.
- Address a rare issue that would occur during installation of versions 3.1.5-3.1.8.

6 March 2014 Release Notes

AMP for Endpoints Console v4.5.20140306

New

- Two-Step Verification will be an available option for all users.

Bugfixes / Enhancements

- Detailed file information can now be accessed from the File Trajectory page either by search or by right-clicking the filename or SHA-256 value.
- A single default exclusion set is now created during first use rather than one each for Audit, Protect, and Triage policies.
- Address an issue where policy scheduled scans created in the month of January would fail to run.
- New favicon for the AMP for Endpoints console.
- Added new Indication of Compromise event called Generic IOC to flag suspicious behavior.

23 January 2014 Release Notes

AMP for Endpoints Console v4.5.20140123

New

- AMP for Endpoints First Use wizard is now available to new businesses on first login.

Bugfixes / Enhancements

- Improved search including better filename identification and direct linking to device trajectory when searching.
- Detailed file information can now be accessed from the File Trajectory page either by search or by right-clicking on the filename or SHA-256.
- Policy settings to reduce network traffic from Connector updates and TETRA content downloads.
- Address an issue where demo data was being created with a timestamp of midnight and IOC events were not showing up within the hour.
- Numerous cosmetic and validation fixes for users of all browser types across various pages.
- Upgrade to latest version of Ruby on Rails to address security vulnerabilities.

AMP for Endpoints Cloud IOC Engine

New

- Ability for VRT and AMP for Endpoints engineers to create and express new IOCs in the back office.

17 December 2013 Release Notes

AMP for Endpoints Console v4.4.20131212

New

- Beta - Redesigned search page to allow much richer content across both sandbox analysis reports as well as trajectories, groups, policies, and user.

Bugfixes / Enhancements

- Redesigned right-click menu for better design consistency with the rest of the console.

21 November 2013 Release Notes

AMP for Endpoints Console v4.4.20131121

New

- A new section under the Analysis menu item entitled "Prevalence". Prevalence is an events view of obscure executables in a customer environment to allows for better focus on possible unknown threat vectors that would otherwise be difficult to surface.
- A hidden view of the AMP for Endpoints First Use wizard to provide the sales engineering teams an opportunity to provide feedback before it is released to customers.

Bugfixes / Enhancements

- Context sensitivity to the help documentation from the October 24 release making it simpler for customers to find pertinent information quickly.
- Errors encountered during download of connectors now provides an error message to the user.
- Fixed typo on Policy Update Failed event.
- Exclusion paths now handle Yen and Won characters.
- Add informative message to IOC widget for when there are no indications of compromise.
- Fix javascript issue when choosing to deploy connectors via email.

- Address a possible XSS attack using the hostname on the dashboard events page.

30 October 2013 Release Notes

Windows Connector 3.1.6.9505

Bugfixes / Enhancements

- Fixed a typo in the error message shown to users during a failed scan.
- Help shortcut removed from the WIndows Start Menu and Connector UI as it is no longer required.
- Fixed an inconsistent detection behavior related to detecting files via SHA- 256 and ETHOS.
- Addressed a memory leak in DFC that could occur on 64-bit computers.
- Fixed an issue where exclusions were being ignored when running a custom scan of a drive root directory.
- Addressed a rare issue with NetMotion VPN clients where DFC would prevent it from connecting successfully.
- Fixed a rare case where LMS.exe would sometimes crash after the Windows Connector was installed.
- Addressed a case where missing data would cause Device Trajectory to display an empty file path.

24 October 2013 Release Notes

AMP for Endpoints Console v4.4.20131024

Bugfixes / Enhancements

- Made existing help documentation fully indexed and searchable. Please note that it is accessible from the same locations as before and is in the same format.
- Fixed an issue with Device Trajectory in which the right-click menu would always show an unknown disposition even if an item had been identified as malicious or clean.
- Fixed errant removal of DFC Detection event types from the event filter list.
- Address two rare javascript issues that were causing device trajectory to load slowly or incorrectly
- Fixed an issue where pagination of simple custom detection lists could result in a 500 error

4 October 2013 Release Notes

AMP for Endpoints Console v4.4.2013092717

New

- Deployment summary page has been redesigned to allow sorting and export of installation status for Windows connectors
- Faster overall experience due to backend software infrastructure upgrades

Bugfixes / Enhancements

- Neutral dispositions have been renamed to Unknown on Device and File Trajectory pages for consistent nomenclature with the Defense Center
- Fix for scenario where deletion of an exclusion set associated with a policy would result in no exclusions for the policy
- Address a javascript error where detection information would not show for move events
- Product update interval in policy has been changed to 60 minutes from 24 hours to allow for more timely Windows connector product updates
- Fix a rare issue with all zero SHA256 would display under Analysis > Events
- Fix for issue where duplicate connectors would show in the console when performing an identity sync by MAC address

27 August 2013 Release Notes

AMP for Endpoints Console v 4.4.2013082215

Bugfixes / Enhancements

- Address an issue where searching for a valid SHA256 would not return a file analysis report
- Fix for case where events would not be rendered when parent SHA for indicator of compromise had no disposition
- Fix for colliding defense center authorizations in rare instances where DC was registered without a valid FQDN
- Fix a rare issue where device trajectory would not render for computers sending up certain filenames
- Users are now notified when copying a policy that has a product update window that occurs in the past
- Allow users to now specify a subscription type when an event filter is created
- Allow sending of filename and path information for Windows connectors to be changed via policy

29 July 2013 Release Notes

AMP for Endpoints Console v4.4.2013072618

New

- Windows connector filenames and paths are now present in Device and File Trajectory when available
- Wildcard exclusions are now available in addition to the current, threat, path, and file extension exclusions
- Events filters can now be selected in their logical groupings to save time when using filters

Bugfixes / Enhancements

- Scheduled scan events have been added as event types that can be filtered on
- Events listing on computers page has been replaced with a button that filters events to the chosen computer on the dashboard page
- Address an issue with the heatmap where subgroups containing computers were not always displayed
- Fix for comments always showing zero on one of the event icons
- Fix for Last Modified field not being updated when changes were made to an existing user
- Address an issue where uploading a valid DFC blacklist would fail erroneously

19 July 2013 Release Notes

Windows Connector 3.1.5.9394

Bugfixes / Enhancements

- Tray icon UI will now shows three states: Connected, Disconnected, and Service Stopped. Previously only Connected and Disconnected were shown.
- Fix driver issue where under certain conditions upgrading from 3.0.6 under Windows XP would not succeed
- Address a race condition where flash scans would not start immediately after connector registration
- Fix an issue in which the UI would show “Disconnected” when connector was running under an account with User privileges only
- Address an issue on Windows XP where network information was not sent at start of connector install
- Fixed a rare condition where connector would show as “Disconnected” on Windows 8

27 June 2013 Release Notes

AMP for Endpoints Console v4.4.2013062716

New

- Event filtering now enabled for all AMP for Endpoints event types
- Full redesign of event subscriptions including subscription emails to provide more pertinent information

Bugfixes / Enhancements

- Heatmap now provides ability to drill down to the group in question and shows detections for the last 7 days
- AMP for Endpoints installer now incorporates the group name into the installer name
- Previously saved event filters can now be renamed
- Addressed an issue where the heatmap was showing detections for inactive connectors
- File Analysis, quarantine restore to all computers available from each event
- Top level event buttons added for File and Device Trajectory

30 May 2013 Release Notes

Windows Connector 3.1.4

New

- Full Windows 8 support
- Updated Tetra engine for all supported OSes

Bugfixes / Enhancements

- New command line switch /contextmenu to disable right-click menu scanning
- Fixed an issue where installation could fail if another installation was already in progress
- Address a defect where installation was enabled for unsupported OSes
- Fix for issue where rootkit removal never completes and no prompt for removal is given
- Fix for CSIDL exclusions not being honored without restart of connector
- Agent.exe renamed to sfc.exe
- Multiple fixes related to installation in proxied environments

AMP for Endpoints Console v4.4.20130530

New

- Functionality to save and create persistent filters for dashboard events

Bugfixes / Enhancements

- Added ability to download policy as XML
- Simple custom detections, application blocking lists, and whitelists can now be renamed
- Addressed an issue where clicking “Create Policy” quickly in succession would result in a silent failure

06 May 2013 Release Notes

AMP for Endpoints Console v4.4.2013050623

New

- Added ability to copy an existing policy
- Disposition of the process involved in a DFC event is now displayed where available

Bugfixes / Enhancements

- Fixed an issue where a silent failure could occur when updating an existing custom exclusion
- Addressed an issue that could occur when paginating on trajectory search page in Chrome and Internet Explorer

Synthetic Events

New

- Recently added IOC “Suspicious botnet” to identify infections based on a variety of characteristics such as port and DGA (domain generation algorithm) used

08 March 2013 Release Notes

AMP for Endpoints Console v4.4.2013030807

New

- Alternate list view now available for dashboard events

- Ability to add comments to individual events in new dashboard list view
- Additional IOCs added for dashboard, event, and trajectory views

Bugfixes / Enhancements

- Nanosecond timestamps now supported in Device Trajectory for better ordering of events in some cases
- Fixed DFC IP lists not succeeding for more than two IP addresses in rare instances
- Various minor cosmetic and javascript issues in Device Trajectory addressed

Windows Connector 3.1.1.9252

Bugfixes / Enhancements

- Fix to ensure completion of Connector upgrades in rare cases where a partial upgrade state previously occurred
- Correct a race condition between Connector startup and uninstalled
- Addressed a failure to find previous Connector versions when upgrading with version check flag

Synthetic Events

New

- IOCs added for the following programs executing unknown applications, which in turn launched a command shell
  - Java
  - Acrobat
  - Word
  - Excel
  - PowerPoint

Bugfixes / Enhancements

- SHAs added to improve efficacy of existing IOCs

08 April 2013 Release Notes

AMP for Endpoints Console v4.4.2013040823

New

- Completely redesigned Threat Root Cause with greatly increased performance
- Email notifications have been redesigned to include richer and more actionable data
- Events can now be exported as CSV from the dashboard event pages

Bugfixes / Enhancements

- Clicking an Indication of Compromise (IOC) from the dashboard widget now takes you directly to the highlighted synthetic event in Device Trajectory
- There is a slidable time scale now available in Device Trajectory allowing users to specify the slice of time they wish to view
- Various bugs addressed in policies, identity sync, and general usage based on customer feedback

Synthetic Events

New

- New IOC to identify computers where malware has been executed

Bugfixes / Enhancements

- New SHAs added to improve efficacy of existing IOCs in field